Paygety OÜ

THE RULES OF PROCEDURE AND RULES OF INTERNAL CONTROL FOR THE CERVICE PROVIDER OF EXCHANGING THE DIGITAL CURRENCY FOR MONEY

For the Implementation of the Money Laundering and Terrorist Financing Prevention Act

Tallinn 2018

GENERAL PROVISIONS AND DEFINITIONS

These Rules of Procedure, hereinafter referred to as the Guide, regulate Paygety OÜ's activities in the implementation of the Money Laundering and Terrorist Financing Prevention Act (Money Laundering).

In this Guide, the following terms have the following meanings:

Money Laundering – Valid definition of money laundering in accordance with § 4 of the Money Laundering Act.

Terrorist Financing – current valid definition according to § 5 of the Money Laundering Act.

Actual Beneficiary – Current Valid Definition in accordance with § 9 of the Money Laundering Act.

Paygety – is a provider of digital currency exchange services who is required to be a person in the sense of the Money Laundering Act.

Business relationship – current valid definition according to § 3 of the Money Laundering Act.

Client – current valid definition according to § 3 of the Money Laundering Act.

Personnel – the Paygety employee, Paygety manager, board members, council members

Contact Person – a person appointed by the management board who is a contact person of the Financial Intelligence Unit. A Paygety board member or other Personnel member may be a contact person.

1. LIABILITY OF IMPLEMENTATION OF THE MONEY LAUNDERING ACT

The Paygety undertakes to comply with these procedural rules as a provider of the service of digital currency exchange in accordance with § 2 (1) 10) of the Money Laundering and Terrorist Financing Prevention Act (hereinafter referred to as the "Money Laundering Act").

The Paygety Board undertakes to ensure that each Personnel member complies with the requirements set out in this Guide, Money Laundering Act and legislation issued on this basis. The Paygety staff members must be familiar with and comply with the legislation and the relevant authorities' instructions and become familiar with the amendments to the legislation and guidelines independently.[1]

> The personnel member is personally responsible for fulfilling the requirements arising from Money Laundering Act and this Guide. Violation of the requirements may result in termination of an employment contract and misdemeanor or criminal punishment.

DUE DILIGENCE MEASURES

1 The Paygety applies the due diligence measures mentioned in the Money Laundering Act to an appropriate and necessary extent, based on the nature of the Paygety's business and the risk level of the participant involved.

2 The Paygety pays the increased attention to the activities and circumstances of a client that refer to money laundering or terrorist financing or which are likely to be linked to money laundering or terrorist financing.

3 Prior to establishing a business relationship with a client, the transaction performance and in the process of the business relationship, the Paygety shall apply the following due diligence measures:

1 Identification of the Client, verification of the submitted information, data storage and updating;

2 identification and verification of the client's identity and representation rights. The scope of the mandate given to the representative must be specified, including whether it is a longer-term

---

[1] Legal acts are available at www.riigiteataja.ee. The Financial Inteligence Unit's guides are available at http://www.politsei.ee/et/organisatsioon/rahapesu/juhendid/.

relationship or only a one-time transaction, and whether the right of representation allows the Paygety to enter into the business relation.

3 Identification of the actual beneficiary;

4 obtaining information about the business relationship and the purpose and nature of the transaction;

5 day-to-day care and vigilance in communication with the client, including tracking of transactions conducted during the business relationship, regular checking of the data used to identify the person, updating relevant documents, data and information, and, if necessary, identifying the source and origin of the funds used in the transaction;

6 Informing the contact person of situations in which the characteristics of the money laundering or terrorist financing may appear in the content of the transaction or in the client's activity and, if possible, failure to execute such transactions.

1 In the application of diligence measures, if this is not done by means of IT tools, the facts to be identified are determined on the basis of the original documents submitted by the client. If the original document cannot be obtained, the notarized, or notarized and officially certified documents may be used, incl. documents approved by the lawyer. A copy of the document must not be relied on if a doubt arises about the compliance of the copy with the original.

IDENTIFICATION OF THE CLIENT

1 The identity of all persons and their agents who enter into a business relationship with the Paygety must be identified. The personal knowledge of the client or his representative or his or her public awareness does not exclude the fulfillment of the obligation established by the Guide.

2 In order to establish a business relationship with a client, a client – natural person, or a client – representative of a legal person – must be identified by means of IT tools. Identification and control of a person's identity shall be performed using a bank link, ID-card, mobile-ID, Smart-ID, etc., agreed means of communication, which are accessible only to the Client or the Client's representative (e.g., @ eesti.ee or other exclusive mail), or / and unique user IDs and authentication tools, established by the Paygety. If the above-mentioned documents or e-identification tools are not available, in the identification of a natural person, a client must provide to the Paygety a copy of identification document with a photo. Before making any transaction, a member of Personnel must

be satisfied beforehand with the identity of the person / representative and the existence of the right of representation.

3 In addition to the provision of clauses 3.2, the client should submit (by e-mail or in a questionnaire on the Exchange platform unless otherwise stated below) the following personal information:

1 Resident natural person:

1. First name and surname;
2. Personal code;
3. name, number, date of issue, name of issuer of the person's identification document;
4. address of residence;
5. occupation or field of activity;
6. contact telephone number, e-mail address.

2 Resident legal entity:

1. Name and registry code of legal entity;
2. Postal address;
3. Field of occupation;
4. contact telephone number, e-mail address;
5. first name and surname, personal code or date of birth (if not given in the registry card);
6. the basis of the right of representation, in the case of an authorized person – a notarized authorization.

The accuracy of the information provided by the representative of a legal person and the existence of the right of representation is checked at Tartu County Court Registry

Office.

3 Non-resident natural person:

1. First name and surname;
2. Personal code and date and place of birth;
3. Name, number, date of issue, name of the issuer of a travel document;
4. address and postal address of the residence;
5. address of location when creating a contact;
6. occupation or field of activity;
7. information as to whether the person is fulfilling or has fulfilled the essential functions of the public authority, or is a close associate or a family member of a performer of the essential functions of public authority (i.e., a person of the national background within the meaning of the Money Laundering Act);
8. contact telephone number and e-mail address;
9. a notarized copy of the travel document's page with a photo, and, if necessary, of a visa or temporary residence permit. A copy must be sent by post.

4 Non-resident legal entity:

1. name and registry code of a legal entity;
2. domicile, name and web-address of the registry in the state of location; the current printouts of

registries, certificates from the tax authorities of CIS and offshore countries;

3. information about actual beneficiary;

4. postal address;

5. place of business address;

6. field of activity;

7. details of the bank account(s);

8. contact telephone number and e-mail address;

9. first name, surname, personal code or date of birth (if not shown in a registry card) of a representative;

10. the basis of the right of representation, in the case of an authorized person, a document certifying the right of representation certified by a notarized or equivalent procedure and certified or approved by a certificate replacing the legalization (apostille), unless otherwise provided by an international agreement. Notarized copies of the afore-mentioned documents must be sent by post.

    If the value of the transaction exceeds EUR 15.000, the client must provide to the Paygety a copy or a statement of his utility bills of their residence / location, which must not be older than three months, and which shows the name and address of the client.

4 In order to verify the information collected, the Personnel member must use the registers available and the information available on the Internet. Data about referees or additional documents may be required for a business with a higher risk profile. If necessary, the Personnel member asks for more detailed information on the company's business, the purpose of the business relationship to be created. In case of doubt, the customer will be questioned on the basis of the data collected, through the contact telephone.

5 For the long-term relationship, the data collected will be checked and, if necessary, updated, at least once every two years.

6 A photocopier of a document certifying identity for a person shall indicate the name of the Paygety's

employee who identified the person, the date of identification and his / her signature. Data collected to identify a person's identity must be recorded in the Paygety's computer system.

4. DISCLOSURE OF THE RISK PROFILE OF THE CLIENT NATURAL PERSON, DETERMINING THE RISK CATEGORY

A member of the personnel is required to identify the client's personal profile and determine the risk category.

Determination of the client natural person's risk category is based on the client's residence and actual beneficiaries. In determining the risk category of non-resident natural persons, it is also considered whether the client is a national background / his / her family member / his close associate. If the customer is a national background / his/her family member / his close associate, then he / she will automatically fall into category III.

1 I category – lower risk category:

resident or non-resident natural person, who is an actual beneficiary him-/herself;

2 II category - average risk category:

non-resident natural person, who is an actual beneficiary him-/herself and who is not of a national background /his/her family member/ his/her close associate;

resident natural person, who is not an actual beneficiary.

4.2.3 III category – higher risk category:

resident and non-resident natural person, who is of a national background / his/her family member/ his/her close associate;

non-resident natural person, who is not an actual beneficiary him-/herself.

4.3. The risk category is determined by a member of the Personnel at the commencement of the customer relationship and during the customer relationship by adding the relevant category to the client's data.

4.3. If the customer falls in the risk category III, the enhanced vigilance measures should be applied (p.10).

When establishing a business relationship with a high-risk category (Category III) customer, the Personnel member will immediately inform the Contact Person by e-mail or telephone, designated by the Management Board.

5. DISCLOSURE OF THE RISK PROFILE OF THE LEGAL ENTITY CLIENT, DETERMINING THE RISK CATEGORY

5.1 When establishing a business relationship, a member of the Paygety Personnel is required to disclose the activity profile of the legal entity client and define a customer risk profile for a legal entity.

The determination of the risk category is based on the location of the legal person, the area of activity, and the transparency of the structure of the management bodies and the owners of the legal entity.

1 I category – lower risk category:

Legal entity registered in the Republic of Estonia, whose field of activity is defined (except for the fishing industry, construction and repair, wholesale trade and storage of fuel, fuel retail trade, wholesale trade in timber, currency and / or payment services, gambling, staking, casino);

A legal entity registered in the EU member-state or Norway, Iceland, Switzerland, whose shares are publicly listed, and the company does not operate in the fishing industry, construction and repair, wholesale and storage of fuel, retailing of fuel, wholesale trade in timber, currency and / or payment services, gambling, staking, casino;

automatically, in a lower-risk category fall the government agencies, insurance institutions and pension funds, resident credit institutions, resident local government, resident central bank, resident social security fund, non-resident central government, non-resident insurance and pension funds, non-resident local government, state social security non-resident, resident private company daughter, financial institution daughter resident / insurance, and pension funds resident.

2 II category - average risk category:

A legal entity registered in the EU member-state or Norway, Iceland, Switzerland, whose shares are not publicly listed, and the company does not operate in the fishing industry, construction and repair, wholesale and storage of fuel, retailing of fuel, wholesale trade in timber, currency and / or payment services, gambling, staking, casino;

Legal entity registered in the Republic of Estonia, whose field of activity is the fishing industry, construction and repair, wholesale trade and storage of fuel, fuel retail trade, wholesale trade in timber, currency and / or payment services, gambling, staking, casino);

A legal entity registered in the EU member-state or Norway, Iceland, Switzerland, whose shares are publicly listed, and the company operates in the fishing industry, construction and repair, wholesale and storage of fuel, retailing of fuel, wholesale trade in timber, currency and / or payment services, gambling, staking, casino;

Legal entity registered in third countries and Liechtenstein whose shares are publicly listed, and the company does not operate in the fishing industry, construction and repair, wholesale and storage of fuel, retailing of fuel, wholesale trade in timber, currency and / or payment services, gambling, staking, casino.

3 III category – higher risk category:

registered in third countries and Liechtenstein legal entity (except for p. iv in subclause 5.2.2);

A legal entity registered in EU member-state or Norway, Iceland, Switzerland, whose shares are not publicly listed, and the company operates in the fishing industry, construction and repair, wholesale and storage of fuel, retailing of fuel, wholesale trade in timber, currency and / or payment services, gambling, staking, casino;

4 If the customer belongs to risk category III, the enhanced diligence measures should be applied (p. 10).

5 The risk category is determined by the Paygety's Personnel member at the start of the customer relationship and during customer relationships by adding the relevant category to the customer data.

6 When establishing a business relationship with a higher risk category (Category III) customer, the employee immediately informs the Contact Person by e-mail or telephone designated by the Management Board. In addition, the Contact person must be informed if the company's business is related to the arms industry, arms sales or brokering.

IDENTIFYING A PERSON DURING THE CUSTOMER RELATIONSHIP

1 Customer identification is required during the customer relationship.

2 The Paygety is entitled to suspend or terminate transactions if, in the event of a suspicion of money laundering revealed during the duration of the business relationship, the client fails to provide

documents or information that would discourage such suspicion. In the case of suspicion of money laundering, a decision to suspend or terminate transactions is made by the Paygety Management or Contact Person.

IDENTIFICATION OF NATIONAL BACKGROUND PERSON AND PERFORMING TRANSACTIONS

1 Persons of a national background are persons listed in § 3 (11) of the Money Laundering Act, who are subdivided into national background persons performing tasks given by national and international organizations.

2 A Contact Person shall be responsible for the identifying national background persons among the Paygety's clients and potential clients unless the Paygety management have designated another person thereof.

3 It is possible to identify a national background person through:

1 customer inquiring;

2 using the existing public or paid databases [2] and the Internet search engines; or

3 by requesting or verifying the data through the websites of the authorities in the customer's home country.

4 The establishment of a business relationship with a national background must be decided by the Paygety's Management Board or Contact Person. If a client has a business relationship and the client turns out to be later or becomes a national background, then it is necessary to inform the Contact Person in writing or in a format that can be reproduced in writing.

LOWER AND HIGHER RISK TRANSACTIONS

1 In conducting a transaction, the Paygety's personnel member must assess the risk of money laundering and terrorist financing and choose the appropriate diligence measures in accordance with

---

[2] E.g., WorldCheck http://www.world-check.com/online/

the Guide and apply them.

2 When assessing the risk of money laundering and terrorist financing, the risk of a client and transaction risk are taken into account.

3 The risk associated with the transaction is considered to be minor if the following circumstances occur simultaneously:

1 the benefits of transaction cannot be realized by the client earlier than one year after the transaction has expired;

2 a transaction is not made as a prompt payment;

3 the agreement does not provide for a customer repurchase clause.

4 The lower risk criteria in the identification and verification of the persons or customers specified in clauses of § 34 (2) 1)- 6) of the Money Laundering and Terrorist Financing Prevention Act the following simultaneous circumstances are considered:

1 identification of a customer is possible on the basis of publicly available information;

2 the customer's ownership and control structure is transparent and permanent;

3 the activities of the customer and his accounting practices are transparent;

4 the customer is accountable and controllable by the executive body of the state or an agency of the contracting state of the European Economic Area, other public authority or a body of the European Community.

5 The customer risk is considered high if the customer:

1 has been entered in the UN or European Union list of persons subject to international financial sanctions [3];

2 person about whom the Payget has a known suspicion that a person may be involved in money

[3] https://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/

laundering or terrorist financing.

6 The risk associated with the transaction is considered to be high if:

1 The transaction is requested by a representative of the customer who cannot reasonably explain the origin of the money;

2 The transaction is intended to be performed by a customer who has previously been suspected by the Paygety that he may be involved in money laundering or terrorist financing;

3 the transaction is requested by cash payment;

4 the transaction is made by making a cash deposit to a third party or through a third party;

5 transactions or operations that meet the characteristics specified in Annexes 2 and 3 to this Guide.

2 In the case of high-risk transactions, diligence measures should be implemented in an enhanced manner.

3 In the event of an unusual transaction, operation or circumstance, the Personnel is required to analyze and compare the circumstances of the transaction with the characteristics of transactions suspicious of money laundering and terrorist financing. A member of the personnel is required to check the legal origin of the property before the transaction is carried out, at least if the transaction is unusual in terms of suspicion of money laundering or terrorist financing, given the current customer relationship.

4 The diligence measures must be implemented in an enhanced manner as well, if there is a suspicion of money laundering or terrorist financing for low-risk transactions or customers.

IMPLEMENTATION OF DUE DILIGENCE MEASURES IN A SIMPLIFIED MANNER

1 The diligence measures may be applied in a simplified manner under the following conditions:

1 For persons specified in § 34 (2) 1) – 6) of the Money Laundering Act; or

2 if the customer has been given a written durability agreement; or

3 if the Personnel member does not suspect the accuracy of the information provided by the

Customer or the Customer's ability to act or his legal capacity; and

4 if the Person does not suspect money laundering or terrorist financing in connection with the transaction; and

5 if the transaction or client risk can be considered low; and

6 in presence of a previous business relationship with the customer, created before the introduction of this Guide, or the customer is identified after the introduction of this Guide in accordance with the Guide,

2 <u>In application of the simplified diligence measures:</u>

1 Persons shall be identified in accordance with clause 3 of this Guide;

3 If the Personnel member, however, encounters doubt as to the accuracy of the information provided by the customer in the application of simplified due diligence measures, the Personnel shall carry out some additional checks. In the course of such additional checks, the Paygety's employee calls the customer and specifies the customer information and may ask other verification questions[4]. If the verification cannot be carried out or the inspection reveals that the customer is not able to answer the verification questions, the transaction with the customer will not be performed.

4 It is prohibited to apply diligence measures in a simplified manner in the case of any suspicion of money laundering or terrorist financing in the stage of communication with the customer. If, in the course of the application of the simplified diligence measure, a Member of the Personnel has a suspicion of money laundering or terrorist financing, the Personnel member informs the Contact Person by telephone or by e-mail.

[4] For instance, customer's e-mail address, postal address, date of birth, personal code and any other data related to the business relation may be requested.

IMPLEMENTATION OF DUE DILIGENCE MEASURES IN AN ENHANCED MANNER

1 A member of the Paygety's personnel applies diligence measures in an enhanced manner if the nature of the situation is accompanied by a high risk of money laundering or terrorist financing. Reinforced diligence measures must be applied when:

the identity of the customer participating in the transaction has been identified and the information submitted has been checked without being present at the same place; and

the identification or verification of the information provided gives rise to doubts as to the accuracy of the information provided or the authenticity of the documents or the identification of the actual beneficiary or actual beneficiaries; and

The customer participating in the transaction is a person of the other Contracting Party to the European Economic Area or a third country national background, his or her family member, or a close associate; and

there are features of transactions with higher risk.

In presence of the obligation to apply an enhanced diligence measure, in addition to the usual due diligence measures one of the following enhanced due diligence measures should be implemented:

i) Identification of the person and verification of the submitted information on the basis of additional documents, data or information derived from a reliable and independent source or from a credit institution incorporated in the commercial register in Estonia or a branch of a foreign credit institution or a credit institution which is registered or has its place of business in a Contracting State of the European Economic Area or in a country subject to equivalent requirements for money laundering and terrorist financing prevention act, and if the identity of the person in that credit institution is identified by the person staying at the same place;

ii) taking additional measures to verify the authenticity of the documents submitted and the accuracy of the information contained therein, including requiring their notarized or formal confirmation or confirmation of the correctness of the data by the issuing institution in point (i);

iii) the first payment of a transaction through an account opened in the name of a participant in a

transaction, with a credit institution registered or whose place of business is in a Contracting Party to the European Economic Area or in a country subject to the requirements equivalent to the Money Laundering and Terrorist Financing Prevention Act.

2 In the event of an unusual transaction, operation or circumstance, the Personnel member is required to analyze and compare the circumstances of the transaction with the characteristics of suspicious transactions in money laundering and terrorist financing. The personnel member has a duty to verify the legal origin of the property before the transaction is executed, at least if the transaction is unusual with the suspicion of money laundering or terrorist financing, given the current customer relationship.

3 For transactions with higher risk, the circumstances of the transaction must be compared with those of suspicious transactions in money laundering or terrorist financing, and the Contact person should be informed of suspicion of money laundering and terrorist financing.

MONITORING BUSINESS RELATIONSHIP

12.1. A Personnel member appointed by the Paygety management undertakes to monitor the business relationship with the client on a regular basis to ensure that the transactions performed correspond to their business and risk profiles. To this end, the Personnel Member undertakes:

Regularly monitor the amount of money used in the transaction and the frequency of transactions, and, if necessary, identify the origin of the assets used in business relationships and / or transactions;

Regularly check the client's legal status (existence of legal capacity), financial situation, field of activity, ownership information (actual beneficiaries).

12.2. Additionally, a Personnel member should monitor at least once a year:
Customer risk assessment;
Assessment of the customer's home country;
Combined risk assessment.
In **the customer risk** (risk factors arising from the customer's identity) the following must be taken into the account:
the legal form of a person, the management structure (including trusts, partnerships or other such contractual legal entities, legal entities with bearer shares);

the ownership structure of the company, in particular, those with no obvious business justification and which can make it easier for the final beneficiary to hide;
the field of activity of a person (customers involved in business activities including the handling of large amounts of cash, such as currency exchange offices, money carriers, dealers of high value goods, casinos, betting and other companies involved in gambling activities who receive regular payments in cash).
whether a person is a national background / his/her family member or close associate (client or beneficial owner);

1) whether the representative of a person is a legal person;

the residence of a person, incl. whether it is a person registered in an *offshore* region (tax-free and low-tax territories, for example, on the basis of the data provided on the website of the Tax and Customs Board http://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest;

circumstances arising from the experience of communicating with the client, its co-operation partners, owners, agents, etc. (for example suspicious transactions detected during the previous business relationship, suspicious behavior of the client, failure to provide the required documents);

2) the duration of the activity, the nature of business relations.

Country risk, the risk factors of which arise from the differences in the legal environment of different countries, the level of crime and the international sanctions imposed or going to be imposed on persons of this or that country.
The most risk-exposed countries include:

countries – subject to international sanctions or embargoes;

lacking sufficient money laundering laws and regulations consistent with international standards;

for which terrorist financing or support has been identified;
for which a significant level of corruption or organized crime or other crime (including drug trafficking) has been identified;
which are tax-free and low-tax, *offshore* financial centers.

Joined, or combined risks

Special attention must be paid by the Personnel member to situations that point to a higher risk in several of the above-mentioned risk groups.

The results of the above-mentioned analysis must be communicated by a Personnel member to the contact person in writing.

COLLECTING, CHECKING, KEEPING AND UPDATING OF DATA

1 Collecting of data

1 The first identification of the customer shall be in accordance with the procedure provided for in clause 3 of the Guide.

2 Every time a customer is identified, the Paygety registers on the computer system / exchange platform:

1 customer name, personal identification code, place of residence [5], activity or profession; and

2 information on the data provided by the customer and on the verification of other data and documents required by the Guide.

2 Checking of data

1 In case of doubt the validity of an identity document should be checked on the website of the Police and Border Guard Board: http://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/index.dot.

3 Collecting and keeping of data

1 The Customer and his representative's data, a copy of the identity document of the customer and its representative, other documents requested from the Customer under the Guide and the Money Laundering Act are stored digitally on the Paygety computer system (server) or on paper at the location of Paygety's management or other place designated by the Management Board for at least 5 years after the ending of the contractual relations with the

---

5 Place of residence is the actual address (place of stay) of a person.

customer.

2 Transaction data relating to suspicion of money laundering or terrorist financing [6] shall be kept by the Contact Person in such a way that other members of the Paygety's Personnel do not have access to such data without the permission of the Contact Person.

3 Information relating to suspicion of money laundering or terrorist financing is retained until the expiration date in clause 14.4.1, except for a case if the investigation of the circumstances surrounding the transaction has not been completed by that time, in which case the customer and transaction data will be retained until confirmation of the termination of the investigation.

4 Updating data and documents, measures of internal control

1 At least once every two years updating of the data must be carried out. In the course of updating the data, a report by a member of the Personnel, appointed by the Management Board, is drawn up, which includes the risks that have been identified in relation to the business, the description of the control measures to mitigate the risks and, if there are any deficiencies, how to deal with them. The report shall be submitted to the Contact Person and the Management.

2 A staff member responsible for customer relationships (customer manager) pays much greater attention to checking the customer risk profile (Category III), identified as a result of the risk analysis and knowing the business activity. In addition to the annual analysis, the Customer Manager must continuously evaluate the potential risks of money laundering and terrorist financing related to the business of the customer and is required to immediately notify the Contact Person of a change in the risk profile.

3 The contact person draws up a detailed monitoring plan based on the report results, under which the Contact person monitors the more risk-exposed transactions and monitors the customer profile.

---

[6] Among others, the description of the details of the suspicious or unusual transaction, the related party, the date of the transaction and the place of the transaction must be kept.

4 The Contact Person will immediately enter the updated data in the Paygety computer system, in which the data is available to all other Personnel members. The contact person organizes involvement of the management in the process of data updating and analyzing and adopts the results of the report as a basis for the entire risk assessment process, the preparation of action plans and counseling the managers in order to decrease risks.

RESTRICTIONS ON TRANSACTIONS

1 The Paygety or a Member of the Personnel is not allowed:

1 Settle in cash;

2 Perform a transaction with a customer whose person has not been identified in accordance with the Guide;

3 Make transactions with anonymous or fictitious persons who use other names or false name.

2 The Paygety and the Personnel Member will refuse to perform a transaction with the client:

1 where suspicion arises to the accuracy of documents or other information on the grounds of the documents or other information provided, and the client does not adequately explain the circumstances giving rise to the suspicion;

2 whose identity or credentials of a representative cannot be established or verified;

3 whose place of residence or occupation or field of activity or profile cannot be identified;

4 who appear to be on the list of the international sanctions implementation or identified by the Financial Intelligence Unit as a lender of money in laundering or terrorist financing suspicious transactions, if such information is disclosed by the Financial Intelligence Unit;

5 for which, in other circumstances, there is a suspicion that a person may be involved in money laundering or terrorist financing.

3 A refusal to make a transaction is registered in the Paygety's computer system.

MONITORING AND ANALYSING OF TRANSACTIONS

1 The Paygety Personal shall monitor and analyze transactions when performing transactions, whether the transaction or the Customer is not related to money laundering or terrorist financing. A list of

suspicions of money laundering or terrorist financing and suspicious and unusual transactions is given in Annexes 2 and 3 to this Guide (Guidelines of the Financial Intelligence Unit "**The indicative guidelines of the Financial Intelligence Unit on money laundering suspicious transaction**" and the Financial Intelligence Unit guide "**The indicative guidelines of the Financial Intelligence Unit on terrorist financing suspicious transaction**").

2 If the client's activity refers to money laundering or terrorist financing, additional information must be requested from the client to clarify the origin of the money. Additional information may be requested orally and / or in writing, but the information received must be registered and linked to the Paygety's computer system with the client's name.

3 The contact person analyzes customer transactions, if necessary, in order to explain the possible involvement of the transaction in money laundering or the possibility of illegal origin of money.

4 The Contact Person responsible for managing the risk assessment of money laundering and terrorist financing must regularly analyze whether the Paygety's business may have risk factors for money laundering and terrorist financing not covered by this Guide.

5 When identifying new risk factors, the Contact Person must prepare:

1 Explanation on how the Paygety should take into account new risk factors in its business and mitigate risks; and

2 Proposal for completing the Guide and a draft of a new Guide.

CONTACT PERSON

1 The contact person is accountable to the management board. The Paygety Board shall inform the FIU of the contact details of the Contact Person and their changes without delay. If the Contact Person is a member of the board, who is the only member of the management board, the Contact is accountable to the shareholders.

2 The contact person has the right to demand from all Personnel members to comply with the obligations provided for in the Guide and to immediately terminate the possible violation.

3 The tasks of the contact person are as follows:

1 Organizing the collection, analysis and archiving of information referring to the unusual transaction

or if there is a suspicion of money laundering or terrorist financing;

2 transmission of information to the Financial Intelligence Unit in the case of suspicion of money laundering or terrorist financing;

3 Checking the names of persons in the list of financial sanctions of the United Nations and the European Union among the Paygety clients and potential clients;

4 To check the compliance with the Money Laundering Act and other legislation at least once a year, and, if necessary, make proposals to the Board for amendments to the Guide;

5 To check the availability of technical resources necessary for complying with the guide and the timely delivery of information;

6 To check compliance with the requirements of the Guide and legislation on the prevention of money laundering and terrorist financing, and to analyze the results of the check and inform the management about the implementation of the Guide;

7 proposals on risk assessment and management of money laundering and terrorist financing;

8 identification of training needs in the field of money laundering and terrorist financing prevention and the training of the Personnel;

9 informing the Financial Intelligence Unit of the transfer of responsibility for the identification of a customer to a third person;

10 guarantee the enforcement of the precepts issued by the FIU and other authorities on the part of the Paygety;

11 Identifying the national background persons among the clients;

12 fulfillment of other obligations related to the requirements of the Money Laundering Act.

4 The contact person has the right to familiarize himself with the documents and other information used as a basis or a preference for the creation of the business relationship.

MEASURES OF THE INTERNAL CONTROL

1 The compliance with money laundering and anti-terrorist financing measures on the part of the Paygety shall be controlled

2 Contact person for the purposes of this Guide and its annexes, as well as for performing the tasks provided for in legislation.

3 In addition, the Contact person shall carry out, at least once a year, an internal check during which he controls:

Compliance of the operations with the diligence obligation in accordance with this guide;

the compliance of registrations with this Guide;

fulfillment of other requirements for the prevention of money laundering and terrorist financing;

The compliance of the business relationship monitoring procedures, based on this Guide, with this Guide,

Compliance with the legislation and the guidelines of the competent authorities;

Training needs of the employees.

A written report will be prepared by the Contact Person on the conduct of the internal control.
The report states:
The purpose of the inspection;
Time of inspection
The name and job title of the controller
Description of the control carried out
Analysis of the results of the inspection or the general conclusions and analysis of the control carried out.
Description of deficiencies and related risks in case of deficiencies.
Time of elimination of defects, recommended measures required to correct deficiencies and time of the follow-up activities. Upon completion of the follow-up, the Contact person shall add the follow-

up analysis to the inspection report and a list of the measures taken to remedy the deficiencies, indicating the actual time spent on the correction of the deficiencies.

4 In the course of ongoing and annual supplementary inspections, the Contact Person is entitled to:

monitor the work of the Personnel and obtain the technical means necessary thereof;

Demand immediate termination of non-compliance with money laundering and anti-terrorist financing requirements;

Make suggestions for eliminating shortcomings identified during the inspection, incl. to amend and supplement the rules of procedure.

IMPLEMENTATION OF THE NOTIFICATION OBLIGATION

1 The personnel member informs the Contact Person of any occurrence of the following situation:

1 of each transaction in which a financial liability of more than EUR 32 000 or an equivalent amount in another currency is settled in cash regardless of whether the transaction is made in a single payment or in a series of interrelated payments;

2 of a money laundering or terrorist financing suspicious transaction. A list of suspicions of money laundering or terrorist financing and suspicious and unusual transactions is given in Annexes 2 and 3 to this Guide (Guidelines of the Financial Intelligence Unit "**The indicative guidelines of the Financial Intelligence Unit on money laundering suspicious transaction**" and the Financial Intelligence Unit guide "**The indicative guidelines of the Financial Intelligence Unit on terrorist financing suspicious transaction**");

3 cases that refer to violation of the Guide by the Paygety;

4 if the client does not submit an identity document despite the demand, information about his place of residence and the field of activity, and, in the case of representation, the document on which the right of representation is based.

2 No person (including a colleague), other than the Contact Person or the Paygety management, may be notified of any suspicion of money laundering or terrorist financing. Informing the client of a notice on money laundering or suspicion of terrorist financing communicated to the Financial

Intelligence Unit thereof is prohibited.

3 Having identified a suspicious transaction of money laundering or terrorist financing, the Contact person analyzes the content of the information received in relation to the client's current transactions and other known information, and, if necessary, asks the Paygety board member, whether it may be a transaction referring to money laundering or terrorist financing.

4 Information on the suspicion of money laundering or terrorist financing transactions shall be kept by the Contact Person in such a way that other employees of the Paygety do not have the access thereof without a written permission of the Contact Person.

5 In identifying a transaction, the characteristics of which indicate money laundering or terrorist financing:

19.5.1. the Contact Person shall promptly notify [7] the FIU of a suspicious transaction in an oral, written or written format. If the message is transmitted orally, the Contact Person will repeat it in writing within the next working day at the latest;

2 the Contact person authorizes the Paygety's employee to complete the transaction after:

the written permission of the Financial Intelligence Unit to execute the transaction; or

consulting the Paygety member of the board if the postponement of the transaction can cause the significant damage, in which case a written notice to the Financial Intelligence Unit will be forwarded immediately after the transaction has been completed.

6 The contact person shall inform the Paygety Board about any notice submitted to the FIU within three working days of the date of the notification.

7 At the request of the Financial Intelligence Unit, the Contact person submits to the FIU additional information on the circumstances of the transaction and the customer about circumstances related to the suspicion of money laundering or terrorist financing, if such information is available to the

7

Paygety.

8 Additional requirements for the fulfillment of the notification obligation in the case of suspicion of money laundering and terrorist financing may arise from the guidelines of the Financial Intelligence Unit which the Contact Person must independently review at least once a year.

9 The Paygety maintains all reports received from the employees about suspicious and unusual transactions for at least 5 years from the date of receipt of the notice, as well as information and other related documents collected for the analysis of these messages and notifications sent to the FIU together with the time of transmission of the notice and the employee's data.

10 In accordance with § 52 (2) of the Money Laundering Act, the obligation to comply with the obligation to notify in good faith in the case of suspicion of money laundering and terrorist financing and the transfer of relevant information to the Financial Intelligence Unit by violating the confidentiality requirement imposed by law or the contract, and the persons who have fulfilled the obligation to notify is not subject to the liability for disclosure of the relevant data, stipulated by law or agreement.

TRAINING AND NOTIFICATION OF THE EMPLOYEES

1 The contact person periodically trains and informs the Paygety's Personnel in order to raise awareness among the employees:

1 regarding typical cases of suspicious and unusual transactions and preventive measures to be implemented.

2 Compliance with legal requirements;

3 Penalties for non-compliance with legal requirements.

2 Upon taking up a new employee, the Contact person or the authorized Paygety's employee introduces the Guide to the new employee and informs the employee about the application of due diligence measures and the requirement of notification in case of suspicion of money laundering.

3 An employee may require from the Contact person the (advanced) training in anti-money laundering and anti-terrorist financing or explaining how to prevent money laundering and terrorist financing in

the Paygety's business.

4 The contact person regularly assesses the training needs of employees in the prevention of money laundering and terrorist financing and submits a report to the management board.

SUPERVISION

1 Compliance with the rules is monitored by the Contact Person. The activities of the Contact Person are supervised by the Management Board, subject to this guide.

2 The contact person must, in particular, monitor the risk assessment and the risk management, the data collection and storage, and the compliance with the reporting requirements. The Board is responsible for supervising the Board of Directors.

3 The Contact person has the right to access the Paygety's computer system, documents and other information for the purpose of performing his / her duties.

4 The contact person has the right to verify whether the Paygety's Personnel members comply with the requirements of money laundering and terrorist financing, and demand the immediate termination of the violations.

5 The Paygety management and Contact Person shall cooperate with the Financial Intelligence Unit by providing the afore-mentioned authority with information on the implementation of the Guide and other relevant circumstances upon request.

Annex 1. The indicative guidelines of the Financial Intelligence Unit on terrorist financing suspicious transaction

Annex 2. The indicative guidelines of the Financial Intelligence Unit on money laundering suspicious transaction

Annex 3. Reviewing the Guide

I have reviewed the Paygety's OÜ Guide on prevention of money laundering and terrorist financing and I undertake to comply with the Guide.

Name and surname	Date	Signature